BUNDESREPUBLIK DEUTSCHLAND

PCT / IB 03 / 05209

14 NOV 2003

REC'D 24 NOV 2003
WIPO PCT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 54 320.8
Anmeldetag:	21. November 2002
Anmelder/Inhaber:	Philips Intellectual Property & Standards GmbH, Hamburg/DE (vormals: Philips Corporate Intellectual Property GmbH)
Bezeichnung:	Schaltungsanordnung mit nicht-flüchtigem Speichermodul und Verfahren zum Ver-/Entschlüsseln von Daten des nicht-flüchtigen Speichermoduls
IPC:	G 06 F, H 04 L

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Faust

A 9161
08/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

BESCHREIBUNG

Schaltungsanordnung mit nicht-flüchtigem Speichermodul und Verfahren zum Ver-/Entschlüsseln von Daten des nicht-flüchtigen Speichermoduls

Die vorliegende Erfindung betrifft eine Schaltungsanordnung zur elektronischen Datenverarbeitung

- mit mindestens einem nicht-flüchtigen Speichermodul zum Speichern von mittels Ver-/Entschlüsseln gegen unberechtigten Zugriff zu schützenden Daten;
- mit mindestens einer dem Speichermodul zugeordneten Speichermodul-Schnittstellenlogik
  - -- zum Adressieren des Speichermoduls,
  - -- zum Schreiben der Daten auf das Speichermodul sowie
  - -- zum Lesen der Daten vom Speichermodul;
- mit mindestens einem Code-R[ead]O[nly]M[emory]-Modul zum Speichern mindestens eines R[ead]O[nly]M[emory]-Codes; und
- mit mindestens einer dem Code-ROM-Modul zugeordneten Code-ROM-Modul-Schnittstellenlogik
  - -- zum Adressieren des Code-ROM-Moduls sowie
  - -- zum Lesen des ROM-Codes vom Code-ROM-Modul.

Die vorliegende Erfindung betrifft des weiteren ein Verfahren zum Ver-/Entschlüsseln von gegen unberechtigten Zugriff zu schützenden Daten mindestens eines nicht-flüchtigen Speichermoduls.

Konventionellerweise werden für die Verschlüsselung bzw. Entschlüsselung von Inhalten eines nicht-flüchtigen Speichermoduls (sogenanntes N[on]V[olatile]-Memory) erforderliche Schlüsselcodes entweder hard-codiert, mittels speziell hierfür instanziierten Fuse-Zellen definiert oder in einem speziell geschützten Bereich des nicht-flüchtigen Speichermoduls selbst abgelegt.

Jede dieser bekannten Vorgehensweisen birgt jedoch Nachteile in sich: So kann bei hard-codierten Schlüsseln kein Wechsel der Schlüsselcodes für verschiedene Controller-Versionen mit unterschiedlichen ROM-Codes erfolgen; bei der flexibleren Definition der Schlüsselcodes in Fuse-Zellen oder im Falle geschützter E[lectrical] E[rasable] P[rogrammable] R[ead]O[nly]M[emory]-Bereiche ist die Schlüssellänge infolge des Zell- bzw. Flächenaufwands begrenzt.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, eine Schaltungsanordnung der eingangs genannten Art sowie ein hierauf bezogenes Ver-/Entschlüsselungsverfahren der eingangs genannten Art so weiterzubilden, dass einerseits ein Wechsel der Schlüsselcodes für verschiedene Controller-Versionen mit unterschiedlichen ROM-Codes erfolgen kann und andererseits die Länge der Schlüsselcodes nicht limitiert ist.

Diese Aufgabe wird durch eine Schaltungsanordnung mit den im Anspruch 1 angegebenen Merkmalen sowie durch ein hierauf bezogenes Ver-/Entschlüsselungsverfahren mit den im Anspruch 6 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen gekennzeichnet.

Gemäß der Lehre der vorliegenden Erfindung wird mithin ein völlig neuartiger Ansatz zum Erzeugen mindestens eines insbesondere langen Schlüssels für die Ver-/Entschlüsselung mindestens eines nicht-flüchtigen Speichermoduls (sogenanntes "N[on]V[olatile]-Memory") aus R[ead]O[nly]M[emory]-Code-Daten, zum Beispiel für eingebettete Sicherheitscontroller ("embedded security controller"), offenbart.

Für diese Ver-/Entschlüsselung des NV-Memory-Moduls wird der Schlüsselcode aus dem dem (Mikro-)Controller zur Verfügung stehenden ROM-Code extrahiert, der aus Sicht des NV-Memory-Moduls eine Konstante ist; auf diese Weise wird ein Schlüsselcode generiert, der mit bis zu einem Byte Schlüssel pro einem Byte plain/cipher-text als relativ lang bezeichnet werden kann.

Gemäß einer besonders erfinderischen Weiterbildung kann das Generieren des Schlüssel(code)s

- entweder durch zum Schreiben bzw. zum Lesen des nicht-flüchtigen Speichermoduls paralleles Auslesen des ROM-Codes aus dem Code-ROM-Modul
- oder durch einmaliges Auslesen bestimmter ROM-Code-Bytes zum Zeitpunkt der sogenannten "reset sequence" und durch Abspeichern dieser ROM-Code-Bytes in mindestens einem Schlüsselregister (sogenanntes "key register"), bis die ROM-Code-Bytes für mindestens eine Schreiboperation bzw. Leseoperation des NV-Memory-Moduls benötigt werden,

erfolgen.

Gemäß einer vorteilhaften Ausgestaltung der vorliegenden Erfindung läßt sich die Qualität des Schlüsselcodes durch ergänzende oder zusätzliche Maßnahmen, wie zum Beispiel durch mindestens eine zusätzliche Adreßabhängigkeit oder durch Verwürfelung mittels mindestens einer Verwürfelungslogik, noch verbessern, was dann der relativ regelmäßigen Struktur von ROM-Codes entgegenwirkt.

In zweckmäßiger Weise ist die vorstehend dargelegte Erfindung methodisch nicht auf bestimmte Ver-/Entschlüsselungsverfahren beschränkt, sondern kann in bezug auf die Schlüssellänge und/oder in bezug auf die Qualität an die jeweiligen Erfordernisse des eingesetzten Verfahrens angepaßt werden.

Durch die doppelte Nutzung des ROM-Codes als Quelle für lange Schlüsselcodes wird die Sicherheit der Verschlüsselung bzw. Entschlüsselung des nicht-flüchtigen Speichermoduls, das heißt des sogenannten "N[on]V[olatile]-Memory" durch größere Schlüssellängen erhöht, ohne daß eine derartige größere Schlüssellänge auch einen entsprechenden zusätzlichen Flächenaufwand für die Speicherung dieser Schlüsselcodes zur Folge hätte.

Des weiteren wird der Fachmann auf dem Gebiet der Kryptologie insbesondere zu schätzen wissen, daß die erfindungsgemäß generierten Schlüsselcodes vom ROM-Code des Code-ROM-Moduls abhängig sind, das heißt sich mit wechselnden ROM-Codes ändern.

Die vorliegende Erfindung betrifft des weiteren einen Mikrocontroller, insbesondere "embedded security controller", aufweisend mindestens eine Datenverarbeitungseinrichtung gemäß der vorstehend dargelegten Art. Dementsprechend kann die vorbeschriebene Methode in bevorzugter Weise zum Beispiel in alle SmartCard-Entwicklungen eingebaut werden.

Die vorliegende Erfindung betrifft schließlich die Verwendung mindestens einer Schaltungsanordnung gemäß der vorstehend dargelegten Art in mindestens einer Chipeinheit, insbesondere in mindestens einem "embedded security controller".

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 sowie dem Anspruch 6 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend anhand des durch Figur 1 veranschaulichten Ausführungsbeispiels näher erläutert.

Es zeigt:

Fig. 1 in schematischer Blockdarstellung ein Ausführungsbeispiel für eine Schaltungsanordnung gemäß der vorliegenden Erfindung, mittels derer das Ver-/Entschlüsselungsverfahren gemäß der vorliegenden Erfindung durchgeführt werden kann.

In Figur 1 ist ein Ausführungsbeispiel einer Schaltungsanordnung 100 zur elektronischen Datenverarbeitung dargestellt; im speziellen ist die Schaltungsanordnung 100 zur Verwendung in einem Mikrocontroller der Art "embedded security controller" vorgesehen.

Diese Schaltungsanordnung 100 weist ein mehrkomponentiges nicht-flüchtiges Speichermodul 10 (sogenanntes "N[on]V[olatile]-Memory") auf, das als E[lectrical] E[rasable] P[rogrammable]R[ead]O[nly]M[emory] ausgebildet ist und mittels dessen Daten gespeichert werden können, die durch Verschlüsseln bzw. Entschlüsseln vor unberechtigtem Zugriff zu schützen sind.

Diesem N[on]V[olatile]-Speichermodul 10 ist eine Speichermodul-Schnittstellenlogik 12 zugeordnet, mittels derer

- das Speichermodul 10 adressiert werden kann
  (--> Bezugszeichen 120a: Adressdaten "ADDR(a:0)" von der Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10),
- das Speichermodul 10 beschrieben werden kann
  (--> Bezugszeichen 120w: Signaldaten "DIN(d:0)" von der Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10) und
- das Speichermodul 10 ausgelesen werden kann
  (--> Bezugszeichen 120r: Signaldaten "DOUT(d:0)" vom Speichermodul 10 zur Speichermodul-Schnittstellenlogik 12).

Des weiteren weist die Schaltungsanordnung 100 ein Code-R[ead]O[nly]M[emory]-Modul 20 zum Speichern und zum Bereitstellen von R[ead]O[nly]M[emory]-Codes auf. Diesem Code-ROM-Modul 20 ist eine Code-ROM-Modul-Schnittstellenlogik 22 zugeordnet, mittels derer

- das Code-ROM-Modul 20 adressiert werden kann
  (--> Bezugszeichen 220a: Adressdaten "A" von der Code-ROM-Modul-Schnittstellenlogik 22 zum Code-ROM-Modul 20) und
- das Code-ROM-Modul 20 ausgelesen werden kann
  (--> Bezugszeichen 220r: ROM-Code-Daten bzw. ROM-Code-Bytes "DO" vom Code-ROM-Modul 20 zur Code-ROM-Modul-Schnittstellenlogik 22).

Die Besonderheit der Schaltungsanordnung 100 gemäß Figur 1 ist nun darin zu sehen, daß die Schlüsselcodes zum Verschlüsseln bzw. zum Entschlüsseln der dem Speichermodul 10 zugeordneten Daten aus dem ROM-Code des Code-ROM-Moduls 20 extrahierbar und generierbar sind.

Hierzu weist die Speichermodul-Schnittstellenlogik 12 eine Ver-/Entschlüsselungslogik 14 mit einer Schlüsseladressierungserzeugungseinheit 16 und mit einem Schlüsselregister 18 auf. Die Schlüsseladressierungserzeugungseinheit 16 ist in diesem Zusammenhang dafür vorgesehen, daß im Falle eines Schreib- oder Lesezugriffs auf das Speichermodul 10 unter Verwendung einer von der C[entral]P[rocessing]U[nit] kommenden Speichermoduladressierung (--> Bezugszeichen C12a: Adreßdaten "CPU NV addr" von der CPU zur Speichermodul-Schnittstellenlogik 12) eine ROM-Schlüsseladressierung (-->Bezugszeichen 162a: ROM-Schlüssel-Adressdaten von der Schlüsseladressierungserzeugungseinheit 16 zu einer Multiplexeinheit 24 der Code-ROM-Modul-Schnittstellenlogik 22) erzeugt wird.

Diese in der Code-ROM-Modul-Schnittstellenlogik 22 integrierte Multiplexeinheit 24 nimmt nicht nur eine ROM-Schlüsseladressierung der Schlüsseladressierungserzeugungseinheit 16 auf, sondern auch die von der CPU kommenden Adressierungsdaten (--> Bezugszeichen C22a: CPU-ROM-Adressdaten "CPU ROM addr" von der CPU zur Multiplexeinheit 24 der Code-ROM-Modul-Schnittstellenlogik 22).

Daraufhin wird mittels der ROM-Schlüsseladressierung der ROM-Code vom Code-ROM-Modul 20 geholt und als Ver-/Entschlüsselungsschlüssel zum Verschlüsseln bzw. Entschlüsseln

- der Adressdaten "CPU NV addr" von der CPU über die Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10
  (--> Bezugszeichen C12a),
- der Signaldaten "CPU NV write data" von der CPU über die Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10

(--> Bezugszeichen C12w) und

- der Signaldaten "CPU NV read data" vom Speichermodul 10 über die Speichermodul-Schnittstellenlogik 12 zur CPU
(--> Bezugszeichen C12r)

verwendet.

Mithin besteht der Kern der vorliegenden Erfindung darin, daß mittels der Schaltungsanordnung 100 gemäß Figur 1 ein Verfahren zum Verschlüsseln bzw. Entschlüsseln von gegen unberechtigten Zugriff zu schützenden Daten des nicht-flüchtigen Speichermoduls 10 durchgeführt werden kann, wobei die dem Speichermodul 10 zugeordneten Daten mittels des vom Code-ROM-Modul 20 bereitgestellten ROM-Codes verschlüsselt bzw. entschlüsselt werden.

Die Qualität des generierten Schlüsselcodes kann durch Verwürfelung mittels einer an sich bekannten (vgl. Druckschrift DE 199 01 829 A1 aus dem Stand der Technik) und in Figur 1 aus Gründen der Übersichtlichkeit der Darstellung nicht explizit gezeigten Verwürfelungslogik noch verbessert werden, was dann der relativ regelmäßigen Struktur der vom Code-ROM-Modul 20 bereitgestellten ROM-Codes entgegenwirkt.

Diese Verwürfelungslogik umfaßt

- eine Vertauschungsstufe zum Vertauschen verschiedenwertiger Bits der der Verwürfelungslogik zugeführten Adreßsignale "ADDR(a:0)" und/oder Datensignale "DIN(d:0)" bzw. "DOUT(d:0)" untereinander,
- eine Invertierungsstufe zum Invertieren der Werte der Bits der Adreßsignale "ADDR(a:0)" und/oder Datensignale "DIN(d:0)" bzw. "DOUT(d:0)", wobei die Vertauschungsstufe und die Invertierungsstufe durch die Verwürfelungsmustersignale gesteuert werden, sowie
- eine Dekodierstufe zum Gewinnen von Steuersignalen für die Vertauschungsstufe und die Invertierungsstufe aus den Verwürfelungsmustersignalen.

Hinsichtlich der Erzeugung des zum Verschlüsseln bzw. Entschlüsseln dienenden Schlüsselcodes werden gemäß der vorliegenden Erfindung grundsätzlich zwei Varianten (i) und (ii) unterschieden:

(i) Erzeugung des Schlüsselcodes parallel zum NV-Memory-Zugriff, das heißt durch Auslesen des ROM-Codes parallel zu einem Schreib-/Auslesezugriff auf das Speichermodul 10:

Hierbei erhält die Ver-/Entschlüsselungslogik 14 im jeweiligen Interface (= Speichermodul-Schnittstellenlogik 12) des NV-Memory 10 direkten Zugriff auf die unverschlüsselten Ausgangsdaten 220r des Code-ROM-Moduls 20.

Parallel zu jedem Schreibzugriff (--> Bezugszeichen 120w) auf das NV-Memory 10 bzw. zu jedem Lesezugriff (--> Bezugszeichen 120r) auf das Seitenregister des NV-Memory 10 wird auch ein Byte des ROM-Codes aus dem Code-ROM-Modul 20 ausgelesen. Die ROM-Code-Adresse 220a, von der ausgelesen wird, wird durch die Schlüsseladressierungserzeugungseinheit 16 der Ver-/Entschlüsselungslogik 14 bestimmt, hat aber eindeutig und wiederholbar für jede NV-Memory-Adresse 120a zu sein.

Für die Verschlüsselung (bei einem Schreibzugriff oder "write access"; Bezugszeichen 120w) bzw. Entschlüsselung (bei einem Lesezugriff oder "read access"; Bezugszeichen 120r) der NV-Memory-Daten "DIN(d:0)" bzw. "DOUT(d:0)" wird dann dieses ROM-Code-Byte als Schlüsselbyte oder als Teil des Schlüsselbytes benutzt, so daß sich im Extremfall ein Schlüsselraum ergibt, der genau denselben Umfang wie der Code-Raum des nicht-flüchtigen Speichermoduls (= N[on]V[olatile]-Memory) 10 aufweist.

(ii) Erzeugung des Schlüsselcodes in der Reset-Phase, das heißt durch einmaliges Auslesen bestimmter ROM-Code-Bytes, insbesondere zum Zeitpunkt der Resetfolge (sogenannte "reset sequence"), und durch Abspeichern dieser ROM-Code-Bytes im Schlüsselregister 18 bis zu einem Schreib-/Auslesezugriff auf das Speichermodul 10, das heißt bis diese ROM-Code-Bytes für eine Schreiboperation bzw. Ausleseoperation des Speichermoduls 10 benötigt werden:

Als Teil der "reset sequence" des Controllers wird eine Anzahl von ROM-Code-Bytes aus dem Code-ROM-Modul 20 ausgelesen und in Schlüsselregistern 18 gespeichert.

Im Falle eines Schreib- bzw. Auslesezugriffs (sogenannter "write access" bzw. "read access") auf das Speichermodul 10 wird der Inhalt dieser Schlüsselregister 18 als Schlüssel oder als Teil des Schlüssels zur Verschlüsselung bzw. Entschlüsselung der NV-Memory-Daten "DIN(d:0)" bzw. "DOUT(d:0)" verwendet.

BEZUGSZEICHENLISTE

100 Schaltungsanordnung zur elektronischen Datenverarbeitung

10 nicht-flüchtiges Speichermodul oder N[on]V[olatile]-Memory

12 Speichermodul-Schnittstellenlogik

14 Ver-/Entschlüsselungslogik der Speichermodul-Schnittstellenlogik 12

16 Schlüsseladressierungserzeugungseinheit der Ver-/Entschlüsselungslogik 14

18 Schlüsselregister der Ver-/Entschlüsselungslogik 14

20 Code-R[ead]O[nly]M[emory]-Modul

22 Code-ROM-Modul-Schnittstellenlogik

24 Multiplexeinheit der Code-ROM-Modul-Schnittstellenlogik 22

120a Adressdaten "ADDR(a:0)" von der Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10

120r Signaldaten "DOUT(d:0)" vom Speichermodul 10 zur Speichermodul-Schnittstellenlogik 12

120w Signaldaten "DIN(d:0)" von der Speichermodul-Schnittstellenlogik 12 zum Speichermodul 10

162a ROM-Schlüssel-Adressdaten von der Schlüsseladressierungserzeugungseinheit 16 zur Multiplexeinheit 24

220a Adressdaten "A" von der Multiplexeinheit 24 zum Code-ROM-Modul 20

220r ROM-Code-Daten bzw. ROM-Code-Bytes "DO" vom Code-ROM-Modul 20 zur Code-ROM-Modul-Schnittstellenlogik 22

C12a Adressdaten "CPU NV addr" von der CPU zur Speichermodul-Schnittstellenlogik 12

C12r Signaldaten "CPU NV read data" von der Speichermodul-Schnittstellenlogik 12 zur CPU

C12w Signaldaten "CPU NV write data" von der CPU zur Speichermodul-Schnittstellenlogik 12

C22a CPU-ROM-Adressdaten "CPU ROM addr" von der CPU zur Multiplexeinheit 24

C22r ROM-Code-Daten "CPU ROM read data" vom Code-ROM-Modul 20 zur CPU

PATENTANSPRÜCHE

1. Schaltungsanordnung (100) zur elektronischen Datenverarbeitung

- mit mindestens einem nicht-flüchtigen Speichermodul (10) zum Speichern von mittels Verschlüsseln bzw. Entschlüsseln gegen unberechtigten Zugriff zu schützenden Daten;
- mit mindestens einer dem Speichermodul (10) zugeordneten Speichermodul-Schnittstellenlogik (12)
  - -- zum Adressieren des Speichermoduls (10) sowie
  - -- zum Schreiben der Daten auf das Speichermodul (10) bzw.
  - -- zum Auslesen der Daten aus dem Speichermodul (10);
- mit mindestens einem Code-R[ead]O[nly]M[emory]-Modul (20) zum Speichern und/oder zum Bereitstellen mindestens eines R[ead]O[nly]M[emory]-Codes; und
- mit mindestens einer dem Code-ROM-Modul (20) zugeordneten Code-ROM-Modul-Schnittstellenlogik (22)
  - -- zum Adressieren des Code-ROM-Moduls (20) sowie
  - -- zum Auslesen des ROM-Codes aus dem Code-ROM-Modul (20),

dadurch gekennzeichnet,

dass mindestens ein Schlüsselcode zum Verschlüsseln bzw. Entschlüsseln der dem Speichermodul (10) zugeordneten Daten aus dem mindestens einen ROM-Code des Code-ROM-Moduls (20) extrahierbar und/oder generierbar ist.

2. Schaltungsanordnung gemäß Anspruch 1,
dadurch gekennzeichnet,
dass die Speichermodul-Schnittstellenlogik (12) mindestens eine Ver-/Entschlüsselungslogik (14)

- mit mindestens einer Schlüsseladressierungserzeugungseinheit (16) und
- mit mindestens einem Schlüsselregister (18)

aufweist.

3. Schaltungsanordnung gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die Code-ROM-Modul-Schnittstellenlogik (22) mindestens eine Multiplexeinheit (24) aufweist.

4. Schaltungsanordnung gemäß mindestens einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass das Speichermodul (10)

- als mindestens ein E[rasable] P[rogrammable]R[ead]O[nly]M[emory],
- als mindestens ein E[lectrical]E[rasable]P[rogrammable]R[ead]O[nly] M[emory]

oder

- als mindestens ein Flash-Speicher

ausgebildet ist.

5. Mikrocontroller, insbesondere "embedded security controller", aufweisend mindestens eine Schaltungsanordnung gemäß mindestens einem der Ansprüche 1 bis 4.

6. Verfahren zum Verschlüsseln bzw. Entschlüsseln von gegen unberechtigten Zugriff zu schützenden Daten mindestens eines nicht-flüchtigen Speichermoduls (10),
dadurch gekennzeichnet,
dass die dem Speichermodul (10) zugeordneten Daten mittels mindestens eines von mindestens einem Code-R[ead]O[nly]M[emory]-Modul (20) bereitgestellten ROM-Codes verschlüsselt bzw. entschlüsselt werden.

7. Verfahren gemäß Anspruch 6,

dadurch gekennzeichnet,

dass der zum Verschlüsseln bzw. Entschlüsseln dienende Schlüsselcode

- durch Auslesen des ROM-Codes parallel zu mindestens einem Zugriff auf das Speichermodul (10), das heißt parallel zu mindestens einer Schreiboperation bzw. Ausleseoperation des Speichermoduls (10) oder
- durch einmaliges Auslesen bestimmter ROM-Code-Bytes, insbesondere zum Zeitpunkt der Resetfolge (sogenannte "reset sequence"), und durch Abspeichern dieser ROM-Code-Bytes in mindestens einem Schlüsselregister (18) bis zu mindestens einem Zugriff auf das Speichermodul (10), das heißt bis diese ROM-Code-Bytes für mindestens eine Schreiboperation bzw. Ausleseoperation des Speichermoduls (10) benötigt werden,

generiert wird.

8. Verfahren gemäß Anspruch 6 oder 7,

dadurch gekennzeichnet,

- dass bei einem Zugriff auf das Speichermodul (10) mittels mindestens einer von mindestens einer C[entral]P[rocessing]U[nit] kommenden Speichermodul-adressierung mindestens eine ROM-Schlüsseladressierung erzeugt wird,
- dass mittels der ROM-Schlüsseladressierung der ROM-Code vom Code-ROM-Modul (20) geholt wird und
- dass der ROM-Code als mindestens ein Ver-/Entschlüsselungsschlüssel zum Verschlüsseln bzw. Entschlüsseln
  - -- der Adressierung des Speichermoduls (10) und/oder
  - -- der auf das Speichermodul (10) zu schreibenden Daten bzw.
  - -- der aus dem Speichermodul (10) auszulesenden Daten

verwendet wird.

9. Verfahren gemäß mindestens einem der Ansprüche 6 bis 8,
dadurch gekennzeichnet,
dass

- die Adressierung des Speichermoduls (10) und/oder
- die auf das Speichermodul (10) zu schreibenden Daten bzw.
- die aus dem Speichermodul (10) auszulesenden Daten

mittels mindestens einer Verwürfelungslogik verwürfelt werden.

10. Verwendung mindestens einer Schaltungsanordnung (100) gemäß mindestens einem der Ansprüche 1 bis 4 in mindestens einer Chipeinheit, insbesondere in mindestens einem "embedded security controller".

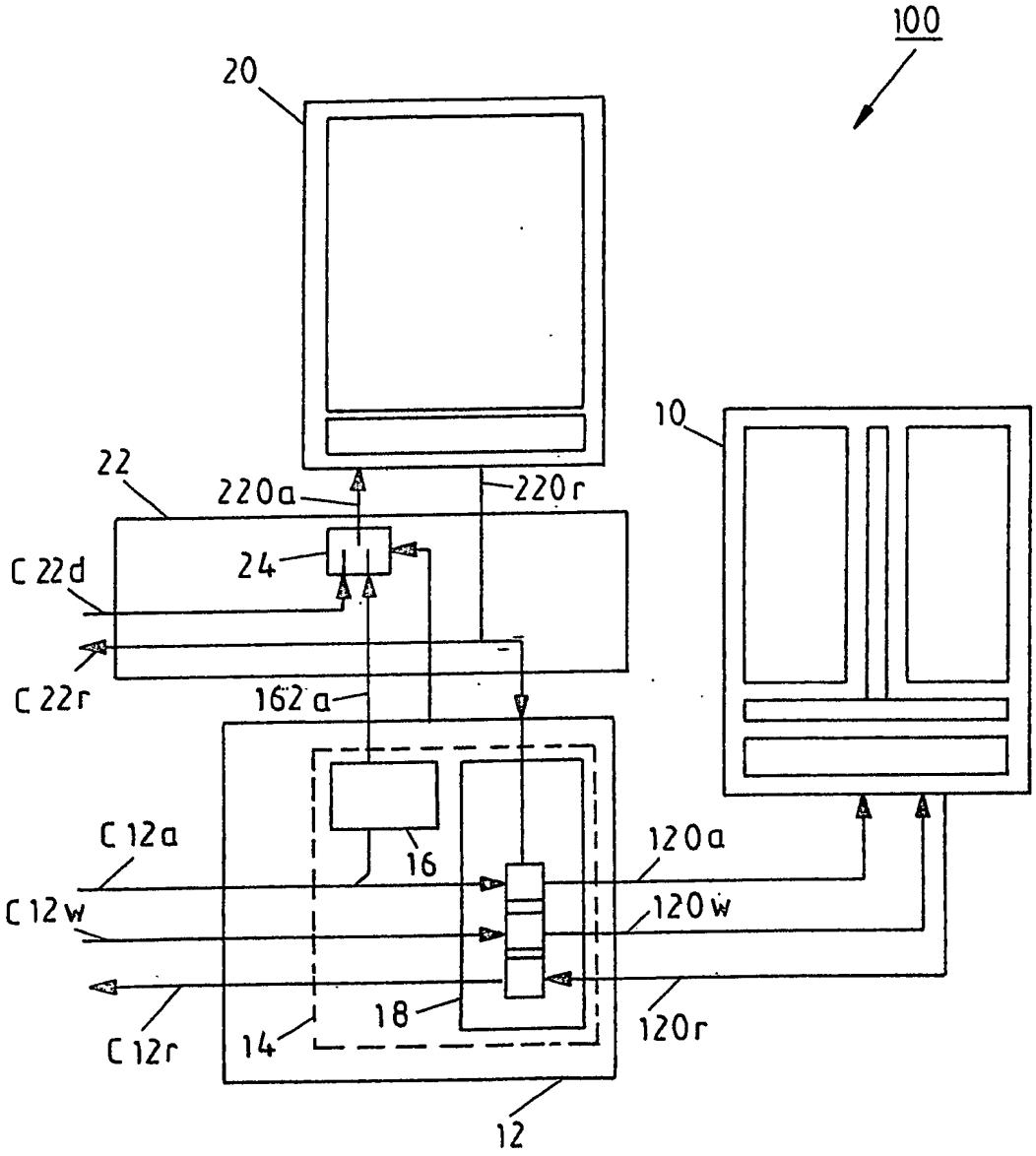
100
20
10
22
220a
220r
24
C 22d
C 22r
162a
C 12a
16
120a
C 12w
120w
18
120r
C 12r
14
12

Fig.1

ZUSAMMENFASSUNG

Schaltungsanordnung mit nicht-flüchtigem Speichermodul und Verfahren zum Ver-/Entschlüsseln von Daten des nicht-flüchtigen Speichermoduls

Um eine Schaltungsanordnung (100) zur elektronischen Datenverarbeitung

- mit mindestens einem nicht-flüchtigen Speichermodul (10) zum Speichern von mittels Verschlüsseln bzw. Entschlüsseln gegen unberechtigten Zugriff zu schützenden Daten;
- mit mindestens einer dem Speichermodul (10) zugeordneten Speichermodul-Schnittstellenlogik (12)
  - -- zum Adressieren des Speichermoduls (10) sowie
  - -- zum Schreiben der Daten auf das Speichermodul (10) bzw.
  - -- zum Auslesen der Daten aus dem Speichermodul (10);
- mit mindestens einem Code-R[ead]O[nly]M[emory]-Modul (20) zum Speichern und/oder zum Bereitstellen mindestens eines R[ead]O[nly]M[emory]-Codes; und
- mit mindestens einer dem Code-ROM-Modul (20) zugeordneten Code-ROM-Modul-Schnittstellenlogik (22)
  - -- zum Adressieren des Code-ROM-Moduls (20) sowie
  - -- zum Auslesen des ROM-Codes aus dem Code-ROM-Modul (20)

sowie ein hierauf bezogenes Ver-/Entschlüsselungsverfahren so weiterzubilden, dass einerseits ein Wechsel der Schlüsselcodes für verschiedene Controller-Versionen mit unterschiedlichen ROM-Codes erfolgen kann und andererseits die Länge der Schlüsselcodes nicht limitiert ist, wird vorgeschlagen, dass die dem Speichermodul (10) zugeordneten Daten mittels des vom Code-ROM-Modul (20) bereitgestellten ROM-Codes verschlüsselt bzw. entschlüsselt werden.

Fig. 1

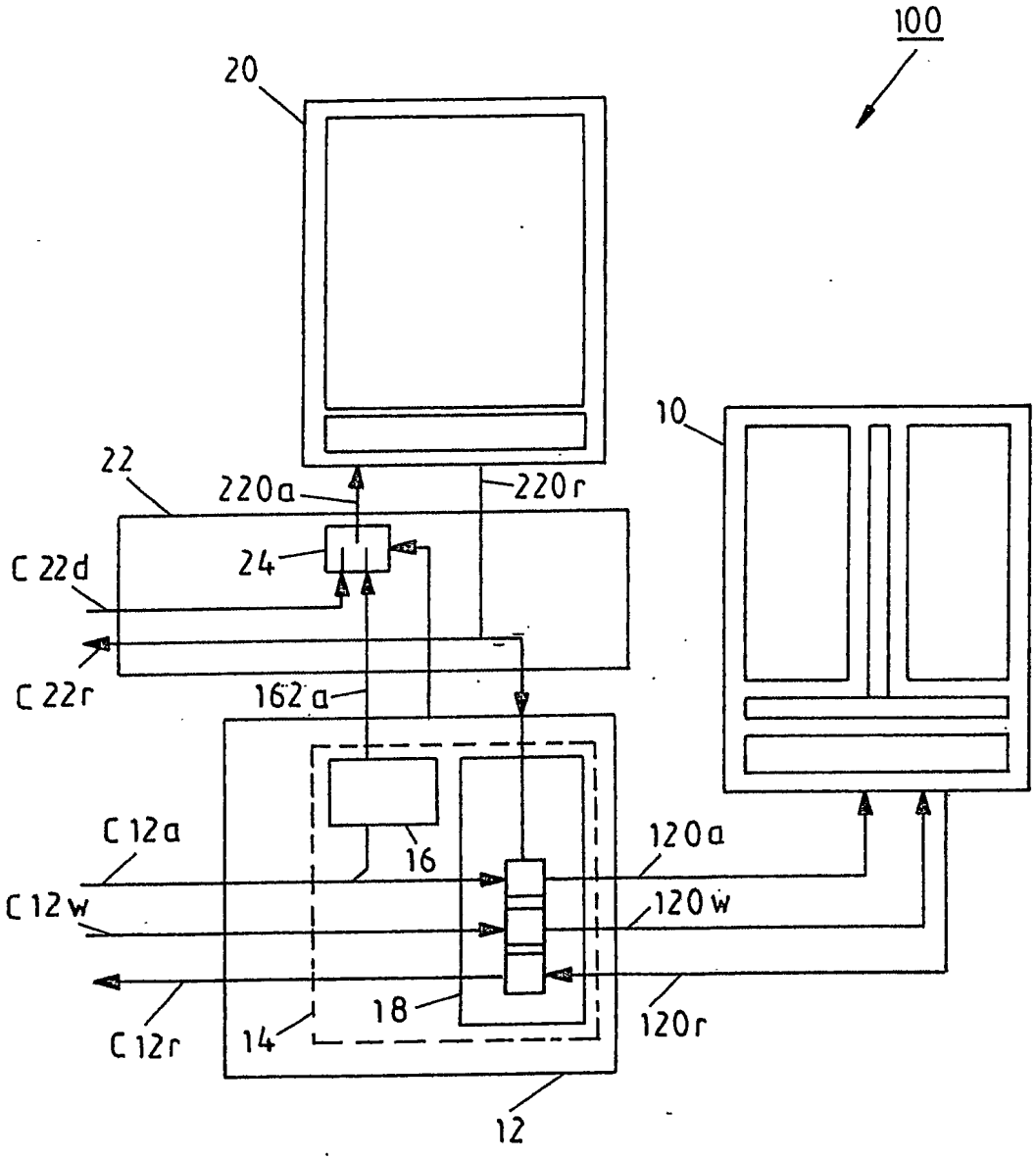
100
20
10
22
220a
220r
24
C 22d
C 22r
162a
16
C 12a
C 12w
C 12r
14
18
120a
120w
120r
12

Fig.1